EXAMINER'S AMENDMENT

1. The application has been amended as follows:

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with applicant's attorney on 10-21-2009.

As per claim 1,

A method, comprising:

executing an authentication protocol, wherein ~~the~~ a terminal authentication protocol comprises

authenticating an identity of a network entity by [[a]] the terminal in a communication system;

sharing a key between the terminal and the network entity for use in securing subsequent communications between the terminal and the network entity; and

executing another authentication protocol comprising

sharing challenge data between the network entity and the terminal;

forming at the terminal test data by applying an authentication function to the challenge data;

sending a message comprising terminal authentication data, from the terminal to the network entity; and

determining, based on the terminal authentication data, whether to provide the terminal with access to a service,

wherein the determining comprises providing the terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key; and

forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the first authentication protocol, wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element.

As per claim 68,

A computer program product embodied on a computer readable storage medium, the computer program product being configured to control a processor to perform a process comprising:

executing an authentication protocol, wherein the authentication protocol comprises

authenticating an identity of a network entity by a terminal in a communication system, and

sharing a key between ~~key~~ the terminal and the network entity for use in securing subsequent communications between the terminal and the network entity; and

executing another authentication protocol comprising

receiving challenge data from the network entity at the terminal;

forming at the terminal test data by applying an authentication function to the challenge data;

sending a message comprising terminal authentication data from the terminal to the network entity;

receiving access to a service at the terminal following a determination of whether the terminal authentication data equals a predetermined function of at least the test data and the session key; and

forming a secret key by at least applying a predetermined function to the test data using the session key, the session key binding the authentication protocol and the another authentication protocol.

Allowable Subject Matter

2. Claims 1-10, 13-20 and 23-69 are allowed.

The following is an examiner's statement of reasons for allowance:

Claims are allowed in the light of applicant's arguments in the Remarks of 07-28-2209, page 25, lines 8-12 and following claim limitations:

As per claim 1,

forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the

first authentication protocol, wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element.

As per claim 18,

forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the first authentication protocol, wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element.

As per claim 26,

forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the first authentication protocol, wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element.

As per claim 36,

forming secret session keys by at least applying a predetermined function to the test data using the shared key established in the first authentication protocol, wherein the secret session keys are configured to secure the

subsequent communications between the terminal and a network element.

As per claim 47,

forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the first authentication protocol, wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element.

As per claim 57,

forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the first authentication protocol, wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element.

As per claim 67,

forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the first authentication protocol, wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element.

As per claim 68,

forming a secret key by at least applying a predetermined function to the test data using the session key, the session key binding the authentication protocol and the another authentication protocol.

As per claim 69,

forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the first authentication protocol, wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 272-7961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/A. S. A./

Examiner, Art Unit 2437

/Matthew B Smithers/
Primary Examiner, Art Unit 2437